INFORMATION ACCESS CONTROLLER AND METHOD

Patent number: JP10222567
Publication date: 1998-08-21

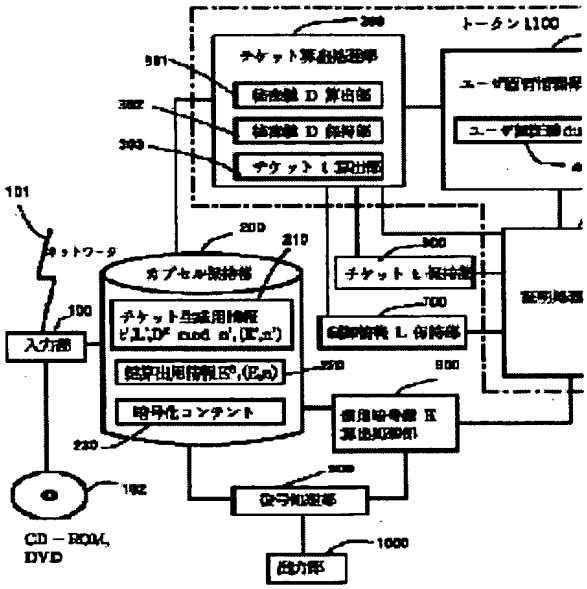
Inventor: MIYAUCHI TADANOBU; KIYOUSHIMA HITOKI
Applicant: FUJI XEROX CO LTD

Classification:
- international: G06F17/60; G06F15/00; G07F7/08; H04L9/08; H04L9/32
- european:
Application number: JP19970024127 19970206
Priority number(s):

Abstract of **JP10222567**

PROBLEM TO BE SOLVED: To independently issue an electronic ticket, maintaining safety in a user's local environment.

SOLUTION: A ticket calculation processing part 300 calculates a ticket t based on ticket creating information that accompanies a content. First, a cryptograph key D calculating part 301 calculates a key of cryptograph D and creates a ticket by using the key D, control information and user's inherent information. The certifying device 500 creates response against a challenge based on the ticket t, the user's inherent information and utilization control information and creates a content decoding key K based on the response. A decoding processing part 900 decodes a content by utilizing the key K.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－222567

(43)公開日　平成10年(1998)８月21日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	17/60		Ｇ０６Ｆ	15/21	Ｚ
	15/00	３３０		15/00	３３０Ｚ
Ｇ０７Ｆ	7/08			15/21	３３０
Ｈ０４Ｌ	9/08				３４０
	9/32		Ｇ０７Ｆ	7/08	Ｒ

審査請求　未請求　請求項の数12　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平9－24127

(22)出願日　平成９年(1997)２月６日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　宮内　忠信
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　京嶋　仁樹
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

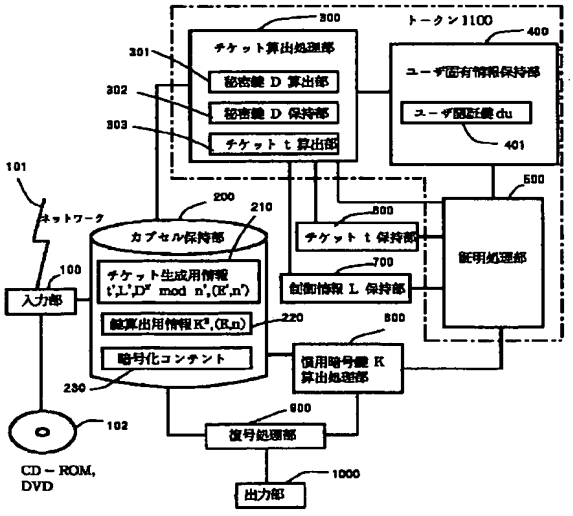
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　情報アクセス制御装置および方法

(57)【要約】

【課題】　利用者のローカルな環境で、安全性を保ったまま独自に電子チケットを発行できるようにする。

【解決手段】　チケット算出処理部３００は、コンテンツに付随するチケット生成用情報に基づき、チケットｔを計算する。まず暗号鍵Ｄ算出部３０１において暗号鍵Ｄを算出し、さらにこの暗号鍵Ｄと制御情報やユーザ固有情報を用いてチケットｔを生成する。この証明装置５００はチケットｔ、ユーザ固有情報、利用制御情報に基づいてチャレンジに対しレスポンスを生成し、このレスポンスに基づいてコンテンツ復号鍵Ｋが生成される。復号処理部９００は鍵Ｋを利用してコンテンツを復号する。



【特許請求の範囲】
【請求項１】　保護対象情報へのアクセスを制御する情報アクセス制御装置において、
ユーザの固有情報を保持する手段と、
上記保護対象情報の管理者から供給される上記保護対象情報の補助情報から上記保護対象情報の固有情報を算出する手段と、
上記保護対象情報の固有情報を保持する手段と、
上記保護対象情報へのアクセス制御用の補助情報を、少なくとも上記ユーザの固有情報および上記保護対象情報の固有情報から算出する手段と、
上記ユーザの固有情報および上記アクセス制御用の補助情報に基づいて上記保護対象情報へのアクセスを許容する手段とを有することを特徴とする情報アクセス制御装置。
【請求項２】　保護対象情報へのアクセスを制御する情報アクセス制御装置において、
ユーザの固有情報を保持する手段と、
保護対象情報の固有情報を保持する手段と、
上記保護対象情報へのアクセス制御用の補助情報を、少なくとも上記ユーザの固有情報および上記保護対象情報の固有情報から算出する手段と、
上記ユーザの固有情報および上記アクセス制御用の補助情報に基づいて上記保護対象情報へのアクセスを許容する手段とを有することを特徴とする情報アクセス制御装置。
【請求項３】　保護対象情報へのアクセスを制御する情報アクセス制御装置において、
ユーザの固有情報を保持する手段と、
上記保護対象情報の管理者から供給される上記情報の補助情報から上記保護対象情報の固有情報を算出する手段と、
上記保護対象情報の固有情報を保持する手段と、
上記保護対象情報の利用制御情報を保持する手段と、
上記保護対象情報へのアクセス制御用の補助情報を、少なくとも上記ユーザの固有情報、上記保護対象情報の固有情報および上記利用制御情報から算出する手段と、
上記ユーザの固有情報、上記利用制御方法および上記アクセス制御用の補助情報に基づいて上記保護対象情報へのアクセスを許容する手段とを有することを特徴とする情報アクセス制御装置。
【請求項４】　上記各手段のうち、少なくとも上記ユーザの固有情報を保持する手段、上記保護対象情報の固有情報を算出する手段、上記保護対象情報の固有情報を保持する手段、および上記保護対象情報へのアクセス制御用の補助情報を生成する手段が、各種情報の保持、伝達および処理の過程で上記各種情報が外部に漏洩するのを防止する防御手段を有する請求項１または２記載の情報アクセス制御装置。
【請求項５】　上記保護対象情報の補助情報は上記保護対象情報の固有情報を所定の方法で暗号化して生成されたものであり、上記保護対象情報の固有情報を算出する手段は、上記保護対象情報の補助情報を復号する手段を含む請求項１、２、３または４記載の情報アクセス制御装置。
【請求項６】　上記保護対象情報は、ＲＳＡ公開鍵暗号の法数ｎ、公開鍵Ｅにて暗号化されており、前記保護対象情報の固有情報は、法数ｎのもとでの前記公開鍵Ｅに対応する秘密鍵Ｄである、請求項１、２、３または４記載の情報アクセス制御装置。
【請求項７】　上記保護対象情報の秘密鍵Ｄが、上記公開鍵Ｅおよび法数ｎとは別の公開鍵ペアＥ’、ｎ’で暗号化されている請求項１、２、３、４または５記載の情報アクセス制御装置。
【請求項８】　上記保護対象情報へのアクセスの制御は復号により行われる請求項１、２、３、４、５、６または７記載の情報アクセス制御装置。
【請求項９】　上記保護対象情報へのアクセスの制御は認証に基づいて行われる請求項１、２、３、４、５、６または７記載の情報アクセス制御装置。
【請求項１０】　上記保護対象情報へのアクセスは、アプリケーションを利用することを含む請求項１、２、３、４、５、６、７、８または９記載の情報アクセス制御装置。
【請求項１１】　保護対象情報の補助情報を送出するステップと、
上記保護対象情報の補助情報を受け取るステップと、
ユーザの固有情報を保持するステップと、
上記保護対象情報の補助情報から上記保護対象情報の固有情報を算出するステップと、
上記保護対象情報の固有情報を保持するステップと、
上記保護対象情報へのアクセス制御用の補助情報を、少なくとも上記ユーザの固有情報および上記保護対象情報の固有情報から算出するステップと、
上記ユーザの固有情報および上記アクセス制御用の補助情報に基づいて上記保護対象情報へのアクセスを許容するステップとを有することを特徴とする情報アクセス制御方法。
【請求項１２】　保護対象情報へのアクセスを制御するために用いられるアクセス制御用補助情報を生成するアクセス制御用補助情報生成装置において、
ユーザの固有情報を保持する手段と、
上記保護対象情報の管理者から供給される上記保護対象情報の補助情報から上記保護対象情報の固有情報を算出する手段と、
上記保護対象情報の固有情報を保持する手段と、
上記アクセス制御用補助情報を、少なくとも上記ユーザの固有情報および上記保護対象情報の固有情報から算出する手段とを有することを特徴とするアクセス制御用補助情報生成装置。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、暗号化された情報の復号や使用権の認証等により情報へのアクセス制御を行う手法に関し、とくにアクセス制御を行う際に用いる補助情報の生成技術に関する。
【０００２】
【従来の技術】近年、暗号技術の進歩やネットワークの発展により、多くの電子流通方式が提案されている。電子流通の実現によりもたらされる効用は非常に多岐にわたるが、とくに有効な利用法のひとつとして、電子的なチケットの流通が挙げられる。ここでいうチケットとは、既存の乗車券、入場券のような紙に印刷された昔ながらのものから、ソフトウェアや電子化されたコンテンツの利用権（ライセンス）、使用料のような電子的な世界のものまでを含む。
【０００３】一般的なチケット利用にあたっては、目的とするサービスの選択からはじまり、チケットの購入、支払い、受領、使用といった一連のプロセスが必要である。これらを人手で行うことは販売者にとってもユーザにとっても手間が大きいため、チケットを電子化し、電子的な決済手段と組み合わせてオンラインで処理することが検討されている。
【０００４】たとえば、特開平８－１４７５００号公報に開示される、電子チケット販売・払戻システムおよびその販売・払戻方法では、複数のチケット発行者との電子マネーを介した安全な取り引きを実現する方法を提案している。この方法では、ユーザは、チケット発行者が作成した電子チケットを、遠隔地から電話回線などを通して入手することができる。この方法によれば、電子チケットの偽造もしくは不正複製を防止するとともに、ユーザは復号化手段を持たない端末装置でも電子チケットの内容の確認のみは可能である。
【０００５】ところが、このような方法は、前述のような乗車券、入場券のような昔ながらのチケットとサービスが一対一に対応するものについては、チケットのオンライン発行自体は可能になるが、電子化されたサービスやコンテンツなどの情報（デジタル情報）までをチケットという概念により包括的に扱う場合には制約が大きい。すなわち、ユーザごとに使用回数、期間などの利用制御を変えるような、電子化によるさらなるメリットを享受するためには、その都度利用制御までを含めた別のチケットとして暗号化を行う必要があるなど、手間が大きい。また、電子マネーの利用を前提にしているという制約もある。
【０００６】これに対し、本出願人は、ユーザ固有情報と、ユーザごとに割り当てた使用回数、期間などの利用制御情報とに基づいて情報提供側でチケットを生成し、これをユーザに送り、ユーザ側での情報の利用の制御を行う手法を提案している（特願平８－１９１７５６号）。なお、この出願の説明では、制御用の情報を証明用補助情報と呼んでいるが、広義のチケットとみなせる。この方法によれば、制御情報をデジタル情報と一緒に暗号化して配布する必要がなくなり、しかも制御情報の改ざんがあった場合の安全性を確保している。
【０００７】しかしながら、前述のふたつの方法は、チケットの発行に際し、安全性のためにユーザの環境とは物理的・論理的に隔てられたサービスの提供者などから発行してもらう必要がある。これをサービスやコンテンツごと、すなわちチケットの適用単位ごとに行うことは、手間が大きい。通信回線などを通してオンラインで受け取るようにしたとしても、小額のチケットにおいては現状では通信コストの割合が大きくなるという第一の問題がある。
【０００８】一方、このような電子チケットを用いるシステムにおいては、サービスまたはコンテンツを提供する業者（プロバイダ）がサービスに応じて複数存在し、これとは独立に秘密情報を扱い、チケット発行や課金を行う組織（センターと呼ぶ）を置くことが一般的である。このときセンター側は、たとえばコンテンツの鍵などの秘密情報を持っていることにより、その気になれば原理的にはコンテンツを自由に見ることができてしまう。こうした問題は、プロバイダにとってはセンターに対する心理的不信感となり得る。このことが第二の問題である。
【０００９】
【発明が解決しようとする課題】本発明は、上述の事情を考慮してなされたものであり、前記第一の問題に対応し、ユーザのローカルな環境で、安全性を保ったまま独自に電子チケットを発行できるようにすることを目的とする。
【００１０】また、本発明は、前記第二の問題に対応し、センターがコンテンツを復号できてしまわないように、センターがコンテンツの鍵を知る必要をなくすことを目的としている。
【００１１】
【課題を解決するための手段】本発明によれば、上述の目的を達成するために、保護対象情報へのアクセスを制御する情報アクセス制御装置に、ユーザの固有情報を保持する手段と、上記保護対象情報の管理者から供給される上記保護対象情報の補助情報から上記保護対象情報の固有情報を算出する手段と、上記保護対象情報の固有情報を保持する手段と、上記保護対象情報へのアクセス制御用の補助情報を、少なくとも上記ユーザの固有情報および上記保護対象情報の固有情報から算出する手段と、上記ユーザの固有情報および上記補助情報に基づいて上記保護対象情報へのアクセスを許容する手段とを設けるようにしている。
【００１２】この構成においては、情報アクセス制御装置側でアクセス制御用の補助情報を生成できるので、外

部から頻繁にアクセス用補助情報を入手する必要がなくなる。

【００１３】また、本発明によれば、保護対象情報へのアクセスを制御する情報アクセス制御装置に、ユーザの固有情報を保持する手段と、保護対象情報の固有情報を保持する手段と、上記保護対象情報へのアクセス制御用の補助情報を、少なくとも上記ユーザの固有情報および上記保護対象情報の固有情報から算出する手段と、上記ユーザの固有情報および上記アクセス制御用の補助情報に基づいて上記保護対象情報へのアクセスを許容する手段とを設けるようにしている。

【００１４】この構成においても、情報アクセス制御装置側でアクセス制御用の補助情報を生成できるので、外部から頻繁にアクセス用補助情報を入手する必要がなくなる。

【００１５】また、本発明によれば、上述の目的を達成するために、保護対象情報へのアクセスを制御する情報アクセス制御装置に、ユーザの固有情報を保持する手段と、上記保護対象情報の管理者から供給される上記情報の補助情報から上記保護対象情報の固有情報を算出する手段と、上記保護対象情報の固有情報を保持する手段と、上記保護対象情報の利用制御情報を保持する手段と、上記保護対象情報へのアクセス制御用の補助情報を、少なくとも上記ユーザの固有情報、上記保護対象情報の固有情報および上記利用制御情報から算出する手段と、上記ユーザの固有情報、上記利用制御方法および上記補助情報に基づいて上記保護対象情報へのアクセスを許容する手段とを設けるようにしている。

【００１６】この構成においても、情報アクセス制御装置側でアクセス制御用の補助情報を生成できるので、外部から頻繁にアクセス用補助情報を入手する必要がなくなる。とくに、利用制御情報ごとにアクセス制御用補助情報をやり取りする必要がなく大変便利である。

【００１７】また、上記構成において、上記各手段のうち、少なくとも上記ユーザの固有情報を保持する手段、上記保護対象情報の固有情報を算出する手段、上記保護対象情報の固有情報を保持する手段、および上記保護対象情報へのアクセス制御用の補助情報を生成する手段が、各種情報の保持、伝達および処理の過程で上記各種情報が外部に漏洩するのを防止する防御手段を有するようにしてもよい。

【００１８】また、上記保護対象情報の補助情報は上記保護対象情報の固有情報を所定の方法で暗号化して生成されたものであり、上記保護対象情報の固有情報を算出する手段は、上記保護対象情報の補助情報を復号する手段を含むようにしてもよい。

【００１９】また、上記保護対象情報は、ＲＳＡ公開鍵暗号の法数ｎ、公開鍵Ｅにて暗号化されており、前記保護対象情報の固有情報は、法数ｎのもとでの前記公開鍵Ｅに対応する秘密鍵Ｄとしてもよい。

【００２０】また、上記保護対象情報の秘密鍵Ｄが、上記公開鍵Ｅおよび法数ｎとは別の公開鍵ペアＥ’、ｎ’で暗号化されるようにしてもよい。この場合、センター側で秘密鍵Ｄを保持する必要がなくなる。

【００２１】また、上記保護対象情報へのアクセスの制御は暗号化により行われてもよく、認証に基づいて行われてもよい。

【００２２】また、本発明によれば、上述の目的を達成するために、情報アクセス制御方法において、保護対象情報の補助情報を送出するステップと、上記保護対象情報の補助情報とを受け取るステップと、ユーザの固有情報を保持するステップと、上記保護対象情報の補助情報から上記保護対象情報の固有情報を算出するステップと、上記保護対象情報の固有情報を保持するステップと、上記保護対象情報へのアクセス制御用の補助情報を、少なくとも上記ユーザの固有情報および上記保護対象情報の固有情報から算出するステップと、上記ユーザの固有情報および上記補助情報に基づいて上記保護対象情報へのアクセスを許容するステップとを実行するようにしている。この構成においても、情報アクセス制御装置側でアクセス制御用の補助情報を生成できるので、外部から頻繁にアクセス用補助情報を入手する必要がなくなる。

【００２３】また、本発明によれば、上述の目的を達成するために、保護対象情報へのアクセスを制御するために用いられるアクセス制御用補助情報を生成するアクセス制御用補助情報生成装置に、ユーザの固有情報を保持する手段と、上記保護対象情報の管理者から供給される上記保護対象情報の補助情報から上記保護対象情報の固有情報を算出する手段と、上記保護対象情報の固有情報を保持する手段と、上記アクセス制御用補助情報を、少なくとも上記ユーザの固有情報および上記保護対象情報の固有情報から算出する手段とを設けるようにしている。

【００２４】この構成においても、情報アクセス制御装置側でアクセス制御用の補助情報を生成できるので、外部から頻繁にアクセス用補助情報を入手する必要がなくなる。

【００２５】なお、上述において上記保護対象情報はアプリケーションであってもよく、この発明によれば、保護対象情報のアプリケーションの利用も制御できる。

【００２６】

【発明の実施の態様】

［実施例１］図１は、本発明の実施例１の構成を示す。本実施例では、暗号化されたコンテント（デジタル情報）を復号する際に、あらかじめ定められた複数の制御情報（利用期間、回数など）のうち、任意の条件を持つ利用チケットを、ユーザのローカル環境で発行し、そのチケットの条件のもとでコンテントを復号して利用する場合について説明する。

【0027】図1において、この実施例のデジタル情報アクセス制御装置は、入力部100、カプセル保持部200、チケット算出処理部300、ユーザ固有情報保持部400、証明処理部500、チケットt保持部600、制御情報L保持部700、慣用暗号鍵K算出処理部800、復号処理部900、出力部1000、トークン1100からなる。以下それぞれについて説明する。

【0028】入力部100は、ネットワーク101などによる外部環境との接続や、CD－ROM，DVDなどのローカルなメディア102との接続を持ち、カプセル保持部200にデジタル情報を供給する。

【0029】カプセル保持部200は、安全にコンテントを保護する部分であり、チケット生成用情報210、鍵算出用情報220、慣用暗号により鍵Kで暗号化された暗号化コンテント（実行形式や可視化用データ）230を保持する。

【0030】鍵Kは、RSA公開鍵暗号で暗号化されており、鍵算出用情報220は、RSA公開鍵E、法数n、および暗号化された鍵K^E mod nを保持する。

【0031】チケット生成用情報210は、チケット生成用チケットt'について、チケット生成用公開鍵n'，E'、およびその制御情報L'と、n'，E'により暗号化したRSA秘密鍵$D^{E'}$ mod n'を保持する。

【0032】ユーザ固有情報保持部400は、ユーザを識別するための固有の情報としてユーザ認証鍵dU（401）を保持している。

【0033】制御情報L保持部700は、使用期限や利用回数などの制御情報Lを保持している。この情報はあらかじめプロバイダよりユーザ個人宛てに配布されているものとする。

【0034】チケット算出処理部300は、チケット生成用情報210から入力される情報に基づき、上記RSA公開鍵Eに対応するRSA秘密鍵Dを秘密鍵D算出部301にて算出し、秘密鍵D保持部302に保持する。さらに、少なくともこの秘密鍵D、法数n（222）、制御情報L、およびユーザ認証鍵dU（401）に基づきチケットt算出部303にてチケットtを算出し、チケットt保持部600に格納する。

【0035】証明処理部500は、RSA公開鍵暗号により暗号化されたデジタル情報（チャレンジと呼ぶ：Cで表記する）に対し、ユーザ認証鍵dU（401）、チケット、制御情報に基づく認証を行い、復号結果（レスポンスと呼ぶ：Rと表記する）を返すプログラムである。本実施例においては、チケット算出と鍵算出の両方に用いている。

【0036】チケットt保持部600は、チケット算出処理部300にて得られた結果を保持し、暗号化コンテントを復号して利用する際のチケットtとして用いられる。本実施例では、チケットtの算出式として具体的に次のものを用いる。

【0037】

【数1】t＝D－hash（dU，L）＋ωφ（n）

算出式において、関数hash（）は、ユーザ認証鍵dUおよび制御情報Lを引数として取る一方向性ハッシュ関数であり、ωは乱数であり、φ（n）は法数nのオイラー数である。RSA暗号では、素数p，qが与えられたとき、n＝p・qとして、E・D＝1 mod （p－1）（q－1）となり、オイラー数φ（n）＝（p－1）（q－1）である。

【0038】ここで、ユーザ環境においてはp，qが与えられていないため、オイラー数が不明であるが、前記よりE・D＝1 mod φ（n）であり、適当な倍数αにおいてαφ（n）＝E・D－1となるので、トークンにEを送れば、トークン内でφ（n）の倍数が算出可能である。

【0039】なお、チケットを算出する方法は、秘密鍵Dから、法数n、ユーザ認証鍵dUおよび制御情報Lに依存した演算結果を加減算したものであれば良く、次のように一般化される。

【0040】

【数2】t＝D－f（L，n，dU）

ここでf（　）は一方向性関数である。

【0041】慣用暗号鍵K算出処理部800は、鍵算出用情報220より得られるK^E mod n、EをもとにチャレンジCを計算し、これと前記n，tおよびLに基づいき証明処理部500から得られるレスポンスRにより、慣用暗号鍵Kを算出する。

【0042】復号処理部900では、得られた鍵Kにより暗号化コンテントを復号する。

【0043】出力部1000では、復号化されたコンテントの種類に応じ、実行形式であればプログラムの実行を、可視化コンテントであればビューワ／ブラウザなどによる可視化といった処理を出力とする。

【0044】トークン1100は、少なくとも前記チケット算出処理部300、ユーザ固有情報保持部400、証明処理部500を含み、保持、伝達および処理の過程で情報が外部に漏洩するのを防止する防御手段により保護（タンパープルーフ化）する仕組みである。このチケットを用いる枠組みでは、チケットによるアクセス制御のために、トークンによるタンパープルーフ化がされている必要がある。

【0045】つぎに本実施例の動作について説明する。まず、チケットtがすでに算出され、その後、デジタル情報を復号する動作を、図2に従い説明する。

【0046】まず、証明処理部500の動作について説明する。証明処理部500は、入力としてユーザ認証鍵dU、制御情報L、チャレンジC、チケットtおよび法数nを受け取り、制御情報Lが条件を満たす場合は次の

値を計算する。

【0047】

【数3】$R' = C^{hash(dU,L)} \mod n$

さらに、次の値を計算し、これをレスポンスRとして出力する。

【0048】

【数4】$R = C^{t}R' \mod n$

次に、慣用暗号鍵K算出処理部800の動作について説明する。慣用暗号鍵K算出処理部800では、与えられた$K^{E} \mod n$、（E，n）に加え、セッションごとに乱数rを生成する。慣用暗号鍵Kに乱数rを乗じたものを暗号化したチャレンジCは、次のように表わされる。

【0049】

【数5】$C = r^{E}K^{E} \mod n$

このチャレンジCをほかの既知の引数とともに証明処理部500に入力する。

【0050】Cの計算時にrを乗じているため、証明処理部500より返るレスポンスRに対し次のようにrの逆数を乗ずることで鍵Kが得られる。

【0051】

【数6】$r^{-1}R = r^{-1}rK = K$

以上によりtが算出されていれば慣用暗号鍵Kが得られ、暗号化コンテントが復号できる。

【0052】つぎに、チケットtをローカル環境で生成する方法を述べる。

（1）まず、チケット発行用のチケットt'について、あらかじめ鍵n'，E'，D'、および制御情報L'を用意する。ここでは、プロバイダと別に秘密情報を管理するセンターの存在を前提とし、D'はコンテンツの秘密鍵Dとともに、センターが保持するものとする。

（2）プロバイダは、センターに次の計算で求められるチケット発行用チケットt'および暗号化したDの送付を受ける。

【0053】

【数7】

$t' = D' - hash(L', n') + \phi(n') \quad D^{E'} \mod n'$

（3）プロバイダは、チケット生成用情報として、上記t'、$D^{E'} \mod n'$に加え、L'，E'，n'をコンテンツに付与する。

（4）ユーザの処理装置において、コンテンツに付随するチケット生成用情報に基づき、チケット算出処理部300にてチケットtを計算する。この計算法には、鍵算出処理部301における計算と同様の方法を用いる。これについて図3に従いさらに詳しく説明する。

【0054】公開鍵E'で暗号化された秘密鍵Dを前述の慣用暗号鍵K算出処理におけるKと同様に扱う。すなわち、与えられた$D^{E'} \mod n$、（E'，n'）、乱数rに基づき、チャレンジC'を次のように計算する。

【0055】

【数8】$C' = (r \cdot D)^{E'} \mod n' = r^{E'}D^{E'} \mod n'$

このチャレンジC'に加え、コンテントに付与されているt'，L'を引数とし、鍵算出とまったく同様に証明処理部500を適用する。すると証明処理部500よりレスポンスRが返るので、これに対し次のようにrの逆数を乗ずることで秘密鍵Dが得られる。

【0056】

【数9】$r^{-1}R = r^{-1}rD = D$

ここで、チケットtは前記のように次の計算で求められる。

【0057】

【数10】$t = D - hash(dU, L) + \omega\phi(n)$

Dが得られたことですべての引数が既知となるので、tを算出し、チケット保持部600に格納する。あとは、チケットが既知の場合として説明した処理を行い、コンテントの復号を行う。

【0058】チケットの算出にあたっては秘密鍵Dが中間結果として計算されるため、チケット算出部303もトークン内に含まれる必要がある。

【0059】図2と図3を比較すれば明らかなように、慣用暗号鍵K算出処理部800と証明処理部500との間のやりとりは、秘密鍵D算出部301と証明処理部500との間のやりとりとまったく同一の構成および処理をなす。したがって、証明処理部500だけでなく、鍵算出部301および鍵算出処理部800も実際にはまったく同じプログラムまたはハードウェアを用いることができる。

［実施例2］つぎに本発明の実施例2について説明する。図4は、本発明の実施例2の構成を示す。本実施例では、実施例1においてセンターが保持することを前提としていたコンテントの暗号化に関する秘密鍵Dを、センターが知る必要をなくし、プロバイダが独自にコンテントの鍵を生成できるようにしている。

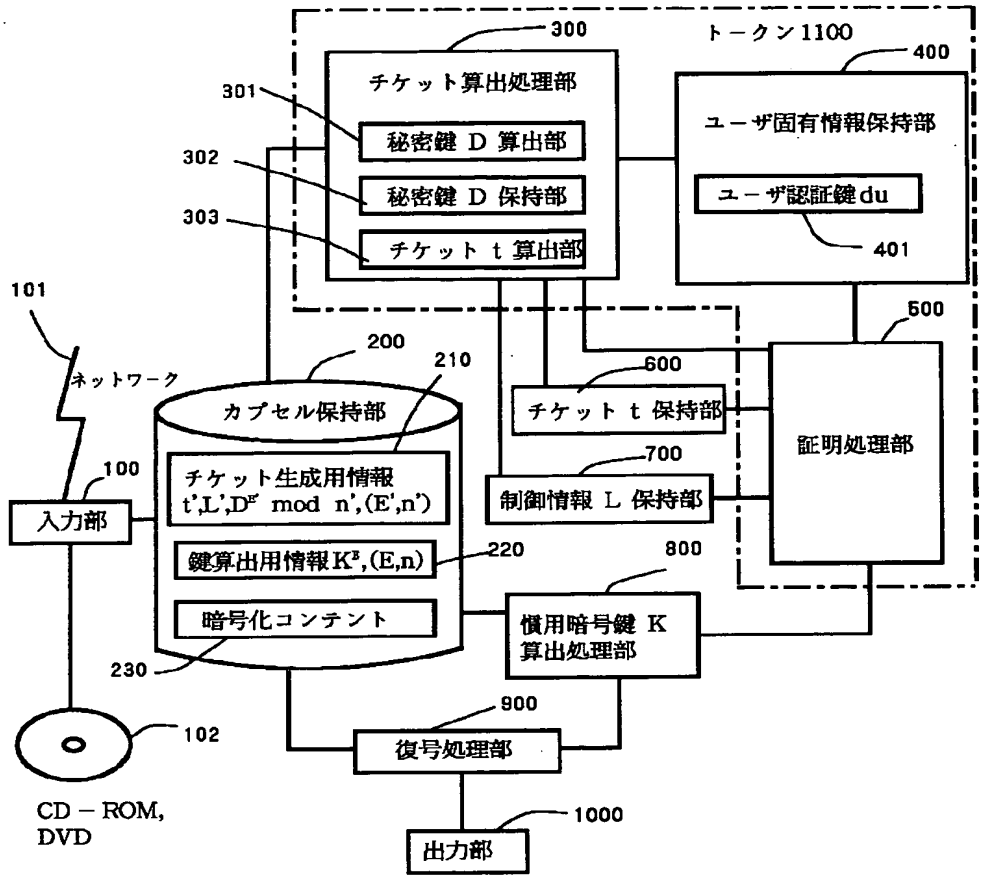
【0060】実施例1と異なるのは、トークンごとに異なるRSA鍵nt，Et，Dtを用いる点である。センターはこれらを管理し、秘密鍵Dそのものは保持しない。また、チケット生成用情報としてチケット発行用のチケットは存在せず、Dを暗号化して受け渡す方法として、前記のRSA公開鍵により暗号化した$D^{Et} \mod nt$を用いる。

【0061】構成上異なるのは、チケット生成用情報210の代わりに暗号化秘密鍵D保持部1200を用意し、ユーザ固有情報保持部400に、トークン秘密鍵Dt（402）、トークン法数nt（402）を保持することである。

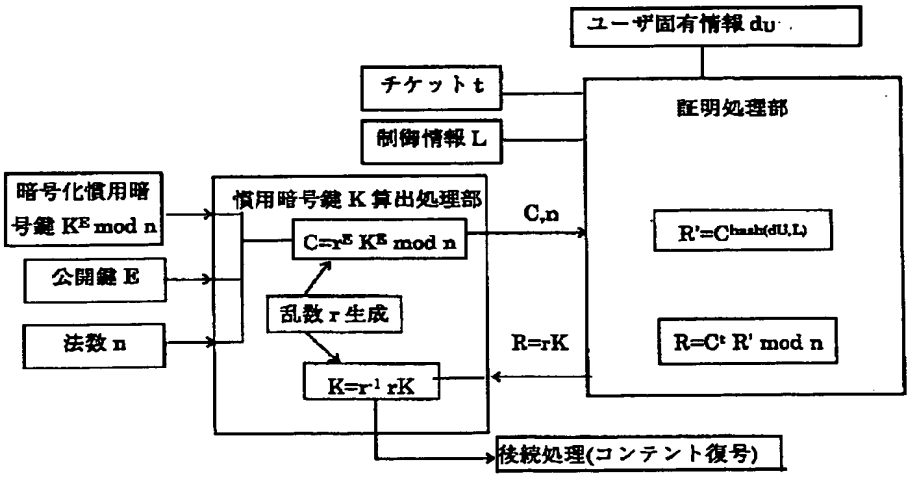
【0062】チケットtを生成してから後の方法は実施例1と同じになるので、ここではチケットtを生成する

方法のみ述べる。
（１）前記のように、センターはトークンごとに異なるＲＳＡ鍵ｎｔ，Ｅｔ，Ｄｔを管理し、トークンにはｎｔ，Ｄｔをタンパプルーフ化して保持する。。
（２）ユーザは、コンテンツのチケット作成に必要なＤ（暗号化したもの）とＬをプロバイダに請求する。
（３）プロバイダは、センターにユーザのトークンのｎｔ，Ｅｔを要求し、暗号化秘密鍵（D^{Et} ｍｏｄ ｎｔ）を計算して、Ｌとともにユーザに送る。
（４）ユーザの処理装置において、暗号化秘密鍵（D^{Et} ｍｏｄ ｎｔ）およびトークン鍵ｎｔ，Ｄｔを用い、チケット算出処理部３００にてチケットｔを計算する。この計算法では、実施例１で述べた鍵算出処理部３０１における計算と類似した方法を用いる。これについて図５に従いさらに詳しく説明する。
【００６３】公開鍵Ｅｔで暗号化された秘密鍵（D^{Et} ｍｏｄ ｎｔ）を前述の慣用暗号鍵Ｋ算出処理におけるＫと同様に扱う。ただし、ここではチケット算出部３００全体がタンパプルーフ化されていることを前提に、乱数ｒは用いない例を示す。なお、これ以外にも、Ｅｔを別途与えるようにして、実施例１で述べたｒを乗じる方法を用いるなど、さまざまな実現が可能である。
【００６４】与えられたD^{Et} ｍｏｄ ｎｔをチャレンジＣｔとする。
【００６５】
【数１１】$Ct = D^{Et} \bmod nt$
トークン内でチケット生成用チケットｔｔを前記と同様に次のように計算する。
【００６６】
【数１２】
ｔｔ＝Ｄｔ－ｈａｓｈ（ｄＵ，Ｌ）＋ωφ（ｎｔ）
このチャレンジＣｔ、ｔｔに加え、プロバイダから送られたＬを証明処理部５００に入力し、レスポンスＲ、すなわち秘密鍵Ｄが得られる。
【００６７】以上により、前記の例と同様にチケットｔを次の計算で求めることができ、あとは通常の復号が可能となる。
【００６８】
【数１３】ｔ＝Ｄ－ｈａｓｈ（ｄＵ，Ｌ）＋ωφ（ｎ）
なおこの発明は上述の実施例に限定されるものでないことはいうまでもない。例えば、上述の実施例におけるチケット算出式は、すでに述べたように、ＤからｄＵ，Ｌ，ｎを引数とした関数を加減算したものであればよく、また、秘密鍵Ｄの算出方法は、実施例２で別の方法について述べたように、外部に漏洩しない方法であればよい。また、上述の実施例では復号鍵Ｋを算出して復号するようにしたが、上述チャレンジおよびレスポンスを利用して認証を行うようにしてもよいことはもちろんである。
【００６９】また本発明はアナログ情報へのアクセス制御例えばアナログ情報へのアクセス権の認証にも用いることができる。
【００７０】
【発明の効果】以上説明したように、本発明によれば、ユーザのローカルな環境で、安全性を保ったまま独自に電子的なチケットを発行できるようにすることができる。これにより、サービスやコンテンツごとにいちいちセンター等を介してチケットの取得を行う必要がなくなり、かつ、小額のチケットにおいては通信コストが不要になるというメリットがある。
【００７１】また、センターがコンテンツを復号できてしまわないように、センターがコンテンツの鍵を知る必要をなくすことができる。これにより、センターがコンテンツを自由に見ることを防ぐことができ、無用な不信感を招くことがなくなる。
【００７２】さらに、実施例に述べたような既存の鍵算出部と証明処理部をいわば二重に適用する実現方法によれば、本発明のために新たに用意する部分は非常に少なくて済み、ハードウェア、ソフトウェアを問わずコストをより低く押さえることが可能となる。とくに、ハードウェアによって実現する場合に低容量化やワンチップ化に有利である。
【図面の簡単な説明】
【図１】　本発明の実施例１の構成を示す図である。
【図２】　実施例１におけるコンテンツの復号動作について説明する図である。
【図３】　実施例１におけるチケット生成動作を説明する図である。
【図４】　本発明の実施例２の構成を示す図である。
【図５】　実施例２におけるチケット生成動作を説明する図である。
【符号の説明】
２００　カプセル保持部
３００　チケット算出処理部
４００　ユーザ固有情報保持部
５００　証明処理部
６００　チケットｔ保持部
７００　制御情報Ｌ保持部
８００　慣用暗号鍵算出処理部
９００　復号部
１１００　トークン

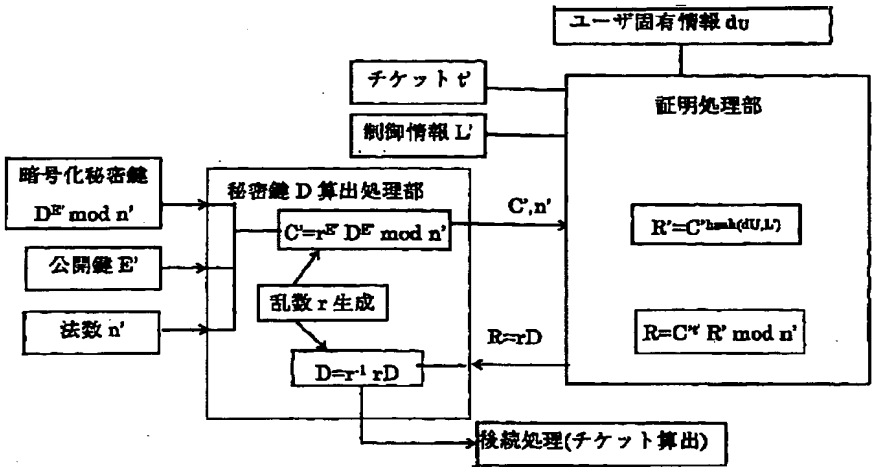
【図１】


300
トークン1100
400
チケット算出処理部
301
秘密鍵 D 算出部
302
秘密鍵 D 保持部
303
チケット t 算出部
ユーザ固有情報保持部
ユーザ認証鍵 du
401
500
101
ネットワーク
200
210
600
カプセル保持部
チケット t 保持部
証明処理部
100
チケット生成用情報
t',L',D^E' mod n',(E',n')
700
制御情報 L 保持部
入力部
鍵算出用情報 K^E,(E,n)
220
800
暗号化コンテント
慣用暗号鍵 K
算出処理部
230
900
102
復号処理部
CD－ROM,
DVD
1000
出力部

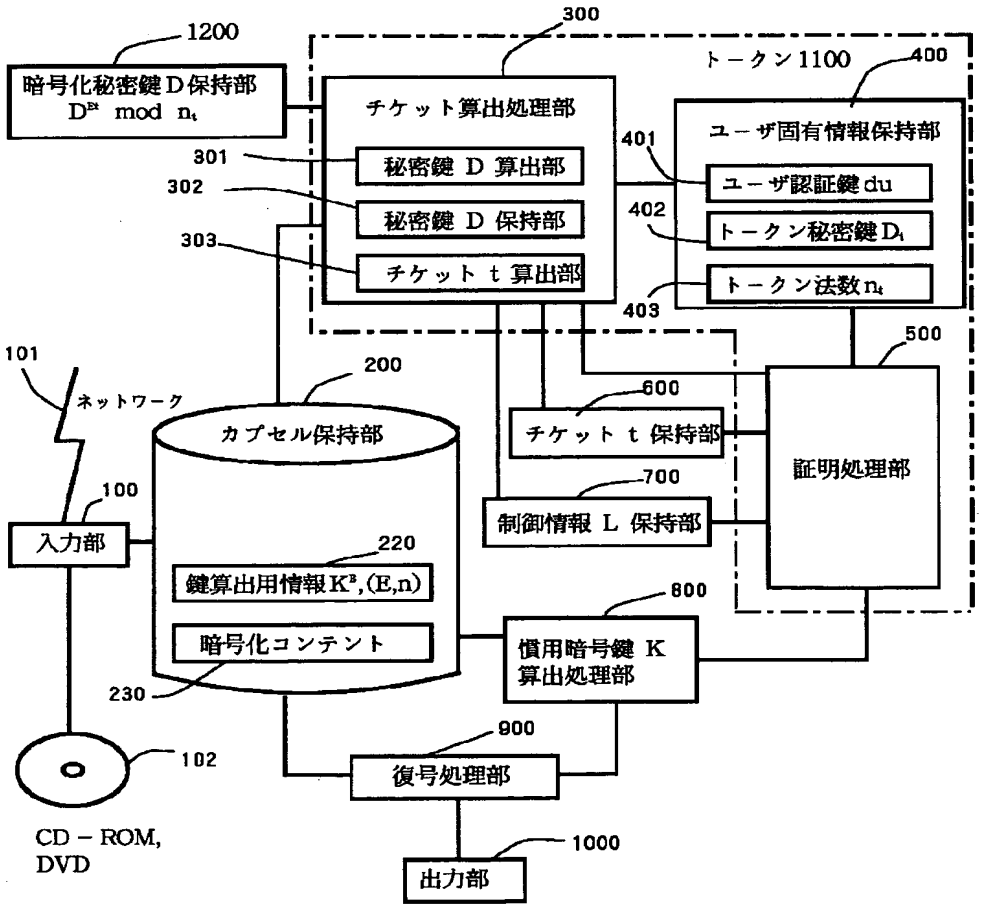
【図２】


ユーザ固有情報 du
チケット t
制御情報 L
証明処理部
暗号化慣用暗号鍵 K^E mod n
慣用暗号鍵 K 算出処理部
C,n
C=r^E K^E mod n
R'=C^hash(dU,L)
公開鍵 E
乱数 r 生成
法数 n
R=rK
R=C^t R' mod n
K=r^-1 rK
後続処理(コンテント復号)

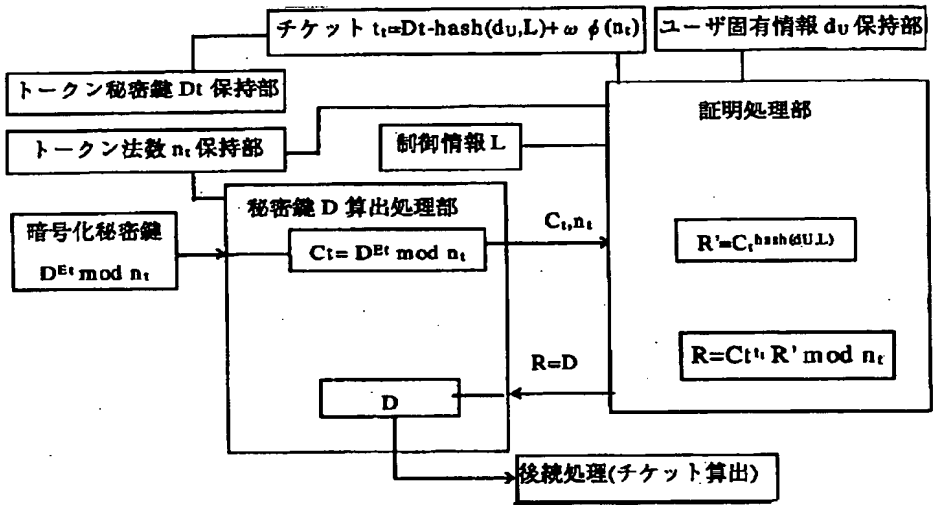
【図３】


ユーザ固有情報 du
チケット t'
制御情報 L'
証明処理部
暗号化秘密鍵
D^E' mod n'
秘密鍵 D 算出処理部
C'=r^E D^E' mod n'
C',n'
R'=C'^h=h(dU,L')
公開鍵 E'
乱数 r 生成
法数 n'
R=rD
R=C'^v R' mod n'
D=r^-1 rD
後続処理(チケット算出)

【図４】


1200
300
トークン1100
400
暗号化秘密鍵 D 保持部
D^Et mod n_t
チケット算出処理部
ユーザ固有情報保持部
401
301
秘密鍵 D 算出部
ユーザ認証鍵 du
302
秘密鍵 D 保持部
402
トークン秘密鍵 D_t
303
チケット t 算出部
トークン法数 n_t
403
500
101
200
ネットワーク
カプセル保持部
600
チケット t 保持部
証明処理部
100
700
入力部
制御情報 L 保持部
220
鍵算出用情報 K^E,(E,n)
800
暗号化コンテント
慣用暗号鍵 K
算出処理部
230
900
102
復号処理部
CD－ROM,
DVD
1000
出力部

【図５】


チケット t_t=Dt-hash(d_U,L)+ω φ(n_t)
ユーザ固有情報 d_U 保持部
トークン秘密鍵 Dt 保持部
トークン法数 n_t 保持部
制御情報 L
証明処理部
秘密鍵 D 算出処理部
暗号化秘密鍵
$D^{Et} \bmod n_t$
$Ct = D^{Et} \bmod n_t$
C_t, n_t
$R' = C_t^{hash(dU,L)}$
$R = Ct^{tt} R' \bmod n_t$
R=D
D
後続処理(チケット算出)

フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
		Ｈ０４Ｌ　9/00	６０１Ｂ
			６０１Ｅ
			６７５Ｂ